IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

CYBERXFORCE CORPORATION and DIGITALXFORCE CORPORATION	§	
Plaintiffs,	§	
v.	§	CIVIL ACTON NO. _____
INSPIRA ENTERPRISE INDIA LIMITED and INSPIRA ENTERPRISE, INC.	§	JURY DEMANDED
Defendants.	§	

PLAINTIFFS' COMPLAINT AND APPLICATION FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY AND PERMANENT INJUNCTION

Plaintiffs CyberXForce Corporation and DigitalXForce Corporation file this complaint and application for temporary restraining order and preliminary and permanent injunction against Defendants Inspira Enterprise India Limited and Inspira Enterprise, Inc. and would show the Court the following:

I. INTRODUCTION

This case involves trade-secret misappropriation, malicious prosecution and wrongful injunction, tortious interference, and business disparagement claims brought against an India-based multinational cybersecurity service provider and its U.S. subsidiary. Defendants violated the Federal Defend Trade Secrets Act (DTSA), 18 U.S.C. § 1836, and the Texas Uniform Trade Secrets Act (TUTSA), TEX. CIV. PRAC. & REM. CODE § 134A.001 *et seq.*, for stealing cybersecurity technology from two U.S. companies.

II. PARTIES

1. Plaintiff CyberXForce Corporation (CyberXForce) is a Delaware corporation with its principal place of business located in Southlake, Texas.

2. Plaintiff DigitalXForce Corporation (DigitalXForce) is a Delaware corporation with its principal place of business located in Southlake, Texas.

3. Defendant Inspira Enterprise, Inc. (Inspira-USA) is a Delaware corporation with its principal place of business located at 1301 Solana Boulevard, Suite 2570, Westlake, Texas 76262 and may be served by and through any of its officers, managing or general agents, or any other agents authorized to receive service of process located at 1301 Solana Boulevard, Suite 2570, Westlake, Texas 76262, or by serving its registered agents—Chetan P. Prakash—located at 2140 East Southlake Boulevard, Suite 803 Southlake, Texas 76092 or National Registered Agents, Inc. located at 1209 Orange Street, Wilmington, Delaware 19801.

4. Defendant Inspira Enterprise India Limited (Inspira-India) is an India private limited company with its principal place of business located at Kalpataru Square, Unit No. 23, Level 2, Kondivita Lane, Andheri East, Mumbai, India 400059. Inspira-India may be served by and through its general agent, Inspira-USA, or Inspira-USA's officers, managing or general agents, or any other agents authorized to receive service of process located at 1301 Solana Boulevard, Suite 2570, Westlake, Texas 76262 or pursuant to the Hague Convention.

5. CyberXForce and DigitalXForce will be referred to collectively as Plaintiffs. Inspira-India and Inspira-USA will be referred to collectively as Defendants.

III. JURISDICTION AND VENUE

6. This Court has federal question jurisdiction under 28 U.S.C. § 1331 for federal trade-secret misappropriation claims brought under 18 U.S.C. § 1836. This Court also has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367 because the state law claims are so related to those claims for which this Court has original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

7. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391. A substantial part of the events or omissions giving rise to the claims occurred within this District, and Defendants are subject to personal jurisdiction in this District.

8. The principal place of business of Inspira-USA is located in Westlake, Texas, and Inspira-USA misappropriated CyberXForce's trade secrets in this District, maliciously prosecuted a lawsuit in this District, wrongfully obtained an injunction in this District, tortiously interfered with Plaintiffs' prospective business relations in this District, and disparaged Plaintiffs in this District, which caused harm to Plaintiffs in this District.

9. This Court has jurisdiction over Inspira-India because the business operations of Inspira-USA and Inspira-India are so intermingled and joined that Inspira-USA is the alter ego of Inspira-India. Inspira-USA was organized and operated as a mere tool or business conduit of Inspira-India. There was such unity between Inspira-India and Inspira-USA that the separateness of Inspira-USA had ceased to exist. Inspira-India has complete control over the operations of Inspira-USA such that Inspira-USA has no separate will or independent existence. Inspira-USA has no independent purpose other than serving Inspira-India's needs and U.S.-based operations.

10. Inspira-India's wrongful conduct took place in Texas when Inspira-India caused Inspira-USA to misappropriate CyberXForce's trade secrets, to disclose those trade secrets to Inspira-India, and to use those trade secrets to sell and offer to sell Inspira-India's services to customers and prospective customers for Inspira-India's benefit and to the detriment of Plaintiffs. Defendants' wrongful conduct caused damage to Plaintiffs in this District.

11. Inspira-USA is a wholly owned subsidiary of Inspira-India. Inspira-India formed Inspira-USA and located its corporate office in Texas for the sole purpose of conducting its U.S.-based business operations. Inspira-USA was formed to conduct a narrow business function for

Inspira-India: A corporate office located in the U.S. to promote and sell Inspira-India's services in North America and elsewhere. As Inspira-India's wholly-owned subsidiary, Inspira-USA acts solely to serve Inspira-India. Inspira-India authorizes Inspira-USA to act on its behalf, and Inspira-USA acts on Inspira-India's behalf.

12. Inspira-USA and Inspira-India have overlapping directors and officers and share the same management team. The Inspira-India board of directors—including Prakash Jain, Vishal Jain and Chetan Jain—govern Inspira-USA. Inspira-India's board members are compensated by Inspira-India for serving on Inspira-USA's board. Inspira-India's board members do not receive any compensation from Inspira-USA to serve on Inspira-USA's board. At all relevant times, Inspira-India and Inspira-USA failed to hold separate board meetings or keep separate minutes. Inspira-India and Inspira-USA routinely disregard their separate legal identities. The Chief Executive Office of Inspira-USA only reports to Inspira-India's board of directors. Inspira-USA submits periodic reports to Inspira-India. Inspira-India's board of directors dominates and directly controls Inspira-USA's management, finances, resources, marketing and the type and quality of its services. Inspira-India is not a holding company; it is the business operating arm and controlling parent company of Inspira-USA.

13. Inspira-India provided Inspira-USA with an initial capital contribution and subsequent capital contributions for its business operations. Inspira-USA, however, is thinly capitalized and is required to routinely request funding from Inspira-India for Inspira-USA's operations. Inspira-India did not document the reasons for Inspira-USA's capital structure. Without a routine infusion of capital from Inspira-India, Inspira-USA would not be able to pay its debts as they came due.

14. The operations of Inspira-India and Inspira-USA are deeply interconnected. Inspira-India and Inspira-USA do not operate independently. Inspira-USA's operations are directly supported by Inspira-India's management and human resources, information technology, marketing, legal, and finance departments. Inspira-India manages Inspira-USA's employment matters, including the hiring and firing of Inspira-USA employees. Inspira-India recruited the Chief Executive Officer of Inspira-USA, who was interviewed and ultimately offered the position by Inspira-India's chairman of the board (Prakash Jain), board members (Vishal Jain and Chetan Jain) and its Chief Legal Officer (Sachin Poptani). Later, Inspira-India's board member (Vishal Jain) and Chief Legal Officer traveled to Texas to fire Inspira-USA's Chief Executive Officer.

15. Inspira-USA and Inspira-India do not have separate books and records. Their finances are managed by the same Inspira-India team and using the same Inspira-India system. All profits from Inspira-USA are distributed to Inspira-India. Inspira-India and Inspira-USA share and exchange the same assets. Inspira-India has access to and directly funds Inspira-USA's bank account. Inspira-India pays for the debts and other financial obligations of Inspira-USA, such as facility expenses, travel reimbursements, and other expenses. Inspira-India and Inspira-USA do not accurately report their dealings with each other in the financial records of either company. Although Inspira-USA uses ADP payroll services, these ADP systems are linked to Inspira-India's human resources department who controls compensation, withholding and benefits for Inspira-USA employees. Inspira-India does not negotiate or conduct its transactions with Inspira-USA at an arm's length, such as intercompany loans, financing, or other transactions. Inspira-India does not separately record or document these intercompany loans, financing, or other transactions. Inspira-India's Chief Legal Counsel is responsible for drafting contracts for Inspira-USA.

16. Inspira-India and Inspira-USA offer the same cybersecurity services to the same types of customers and potential customers. Inspira-India delivers its cybersecurity services to Inspira-USA's customers from delivery centers in Mumbai, Pune, New Delhi and Hyderabad, India. There are over 50 Inspira-India employees whose sole duties are to deliver Inspira-India's cybersecurity services to Inspira-USA's customers. Inspira-India and Inspira-USA use the same cybersecurity control center to manage and monitor their customers' systems, databases and networks against cyber threats. Inspira-US has never operated a control center to independently manage these threats. And Inspira-India never formally authorized Inspira-USA to create a control center for this purpose. If Inspira-USA did not exist, Inspira-India would provide the same services to Inspira-USA's customers and potential customers. In other words, the services provided by Inspira-USA and on behalf of Inspira-India are sufficiently important to Inspira-India that Inspira-India would perform the equivalent services if Inspira-USA did not exist. Inspira-USA sells to customers the right to use Inspira-India's services, even though Inspira-India does not formally authorize Inspira-USA to sell these services. Inspira-USA and Inspira-India have no formal agreements regarding Inspira-USA's right to sell or offer to sell Inspira-India's services, the right to use the INSPIRA brand name, the right to set the price for Inspira-India's services, and Inspira-India's right to set quality standards or seek indemnification from Inspira-USA.

17. Inspira-India and Inspira-USA represent themselves as a "single global entity" to their customers and potential customers. They share the same corporate name—INSPIRA. Inspira-India authorizes Inspira-USA to use the INSPIRA brand name. Inspira-USA, however, does not pay Inspira-India for the use of the INSPIRA brand, which is Inspira-India's trademark. Inspira-USA employees do not differentiate between Inspira-USA and Inspira-India, but rather consistently represent themselves as "Inspira."

18. Inspira-USA holds itself out as being synonymous with Inspira-India. In its dealings with customers and potential customers, Inspira-USA represents that it is the U.S. corporate office of Inspira-India. Inspira-India and Inspira-USA share the same corporate website. They direct their customers and potential customers to the same Inspira-India website at "inspiraenterprise.com." On this website, Inspira-India refers to Inspira-USA as its "North American corporate office." When Inspira-USA salespeople introduce their company, they refer to it as "Inspira Enterprise" without mentioning "Inspira Enterprise, Inc." or any distinction between the two entities. Employees of Inspira-USA and Inspira-India—including Inspira-India's board of directors, its Chief Legal Counsel, and Inspira-USA's Chief Executive Officer—use the exact same "@inspiraenterprise.com" email domain in all their email communications and business cards. Inspira-USA employees use the INSPIRA brand name in their email signature blocks and business cards.

19. Inspira-USA and Inspira-India share the same global practice and solution development teams, including the platform engineering and strategic alliances team that supports the service offering development and engagement delivery for all regions across the world.

20. Based on the foregoing, Inspira-USA is Inspira-India's agent under Texas law when it conducts its business in Texas. Therefore, this principal-agent relationship allows for imputation of Inspira-USA's contacts in Texas to Inspira-India for the purposes of personal jurisdiction. Inspira-India parental control over its agent—Inspira-USA—pervaded Inspira-USA's dealings with the forum and therefore allows Inspira-USA's contacts with Texas to be imputed to Inspira-India for the purpose of personal jurisdiction. Holding only Inspira-USA—a shell company and business conduit for Inspira-India—would result in injustice.

IV. FACTUAL BACKGROUND

A. CyberXForce

21. On November 30, 2022, CyberXForce was formed to be an integrated risk management platform serving customers with automated risk assessments powered by its CyberXForce technology. CyberXForce is located in Southlake, Texas and is owned by Mr. Ahluwalia (Mr. Ahluwalia). Mr. Ahluwalia serves as its Chief Executive Officer.

B. DigitalXForce

22. On April 5, 2023, DigitalXForce was formed to be a digital trust platform providing data-driven, real time, and continuous CyberX Risk Management, that is simplified, measurable, integrated, and actionable. DigitalXForce was designed to be the only platform that can generate a security blueprint, generate security and privacy management plans and procedures, assist with cyber insurance policies, and perform real-time security control analysis by connecting directly with specialty security tools and processes. DigitalXForce is also located in Southlake, Texas and owned by Mr. Ahluwalia. Mr. Ahluwalia serves as its Chief Executive Officer.

C. Lalit Mr. Ahluwalia

23. Mr. Ahluwalia is the Chief Executive Officer of CyberXForce and DigitalXForce. He has a deep and extensive 23-year history in the cybersecurity industry. He graduated as a presidential gold-medalist with a bachelor's degree from Thapar Institute of Engineering and Technology (NIT)—one of the most prestigious and elite engineering universities in India. Mr. Ahluwalia began his career in cybersecurity as an information technology associate at PricewaterhouseCoopers, a $45-billion Big Four accounting firm with worldwide operations. Mr. Ahluwalia was then employed as an enterprise risk services professional at Deloitte and Touche, a $50-billion consulting firm with worldwide operations. While at Deloitte and Touche, Mr.

Ahluwalia was responsible for managing all aspects of projects covering security management, security architecture and strategy, and application security. Later, Mr. Ahluwalia was recruited to work at Accenture, a $60-billion Fortune Global 500 Company, as its North America practice lead for security consulting. He was responsible for over $120-million of cyber security consulting business and managed over 150 security professionals. Mr. Ahluwalia was then employed as a global cyber security head at Wipro, a $10-billion multinational corporation that provides information technology, consultant and business process services.

24. Mr. Ahluwalia is a member of the Forbes technology counsel, an active speaker who presents at various industry conferences—including the National Governors Association—and is the author of numerous articles and whitepapers. He is a highly-regarded thought leader in the cybersecurity industry with an international reputation. Mr. Ahluwalia's passion is to "do business with purpose" and collaborate with other passionate cybersecurity professionals who strive to make a difference in the community. Along the way, Mr. Ahluwalia proudly became a United States citizen and resides with his wife and two sons in Southlake, Texas.

D. The CyberXForce Technology

25. Mr. Ahluwalia invented and created the CyberXForce technology to address the lack of a quantitative and data driven framework that made the cybersecurity ecosystem overly complex, fragmented, and hard to manage. His idea behind the CyberXForce technology was to simply, unify, monetize, and operationalize cybersecurity using an advanced and comprehensive solution to protect a customer's digital assets and maximize return on investment from security investments. The technology he envisioned would automatically identify all the customer's digital assets, identify existing cybersecurity services the customer currently uses, enable new services where gaps in security are found, integrate and analyze current security services, and develop a

security blueprint that establishes security scorecards using industry standards, creates a security plan of action, and operationalizes a cybersecurity plan.

26. In 2020, Mr. Ahluwalia began developing his idea and reducing it to practice. He began working on detailed spreadsheets and data to describe the integrated risk management business logic, technical and operational control assessment logic, asset inventory and attack surface management, security policies and plans review and generation, custom compliance, frameworks, interfaces, security tool connectors, artifacts, modules, source code, instances, security risk controls assessment analysis from NIST CSF and NIST 800-53 control families, and select security control mapping (CyberXForce Technology).

27. To protect the CyberXForce Technology, Mr. Ahluwalia filed a provisional patent application entitled "A2C3 - Advanced & Automated Cyber Command Center" (Application No. 63,018,985) with the United States Patent and Trademark Office (USPTO) on May 1, 2020. A provisional patent application is an application for a utility patent filed in the USPTO under 35 U.S.C. §111(b). A provisional patent application is not required to have formal patent claims. But a provisional application must contain a written description of the invention and comply with all requirements of 35 U.S.C. §112(a). A provisional patent application has a pendency lasting 12 months from the date the provisional application is filed. An applicant who files a provisional application must file a corresponding nonprovisional application for patent during the 12-month pendency period of the provisional application in order to benefit from the earlier filing of the provisional application. A provisional application is automatically abandoned 12 months after its filing date if the applicant does not file a nonprovisional application.

28. An owner may apply for a patent on an invention that comprises a trade secret. Under the Patent Act, patent applications are kept in confidence by the USPTO. 35 U.S.C. § 122(a).

Thus, the public does not know that an inventor has applied for a patent on an invention until the patent issues or in some cases until the patent has been pending for at least 18 months. After filing a patent application, an owner may elect to maintain the idea as a trade secret rather than continue with the prosecution and examination of the patent application.

29. After filing his provisional patent application for the CyberXForce Technology, Mr. Ahluwalia elected to maintain his idea as a trade secret in lieu of continuing with the patent prosecution process. Because Mr. Ahluwalia's provisional patent application was not converted to a nonprovisional application, the USPTO never published the application, and it remained secret.

E. Inspira-India

30. Inspira-India was formed in 2008 as a privately-owned cybersecurity services provider with its principal office located in Mumbai, India. Inspira-India is controlled by a board of directors composed of Prakash Jain, Vishal Jain, and Chetan Jain. Mr. Prakash is the father of Vishal and Chetan Jain.

31. Inspira-India provides cybersecurity services through its various corporate offices located in North America (Westlake, Texas and Toronto, Canada), India (Mumbai, Pune, Jaipur, Bangalore, Chennai, Hyderabad, Kolkata, Navi Mumbai, and New Delhi), Middle East and Africa (Dubai and Abu Dhabi, United Arab Emirates; Riyadh, Saudi Arabia; and Nairobi, Kenya) and the Association of Southeast Asian Nations (ASEAN) (Singapore, Singapore; Jakarta, Indonesia; and Manila and Taguig, Philippines). Inspira-India generates annual revenues of $60 million and now employs 1,500 cybersecurity professionals worldwide.

F. Inspira-USA

32. Inspira-USA was formed on September 11, 2019 as a wholly owned subsidiary of Inspira-India. Inspira-India situated Inspira-USA's corporate office in Texas for the sole purpose of conducting its U.S.-based business operations, including to promote and sell Inspira-India's services in North America and elsewhere. Since Inspira-USA's inception to present, two of Inspira-India's board members—Chetan and Vishal Jain—have served as Inspira-USA's directors. On Inspira-USA's State of Delaware Annual Franchise Tax Report, Messrs. Jain both list their address as Plot 26 Manjul Villa Vithal Nagar Juhu, Mumbai, Maharashstra 4000499, India. As Inspira-India's wholly-owned subsidiary, Inspira-USA acts solely to serve Inspira-India. Inspira-India authorizes Inspira-USA to act on its behalf, and Inspira-USA acts on Inspira-India's behalf.

G. Recruitment and employment of Mr. Ahluwalia by Inspira-India.

33. Inspira-India retained a recruiting firm to recruit qualified candidates to serve as Inspira-USA's Chief Executive Officer and Inspira-India's Global Cybersecurity Head. In early 2022, the recruiting firm introduced Mr. Ahluwalia to Inspira-India. After interviewing Mr. Ahluwalia, Inspira-India offered Mr. Ahluwalia the position.

34. On March 8, 2022, Mr. Ahluwalia and Inspira-USA executed an employment agreement, confidential information and nondisclosure agreement, and a non-competition and non-solicitation agreement. Any disputes related to these agreements or Mr. Ahluwalia's employment with Inspira-USA are governed by an arbitration agreement.

35. Mr. Ahluwalia commenced his employment at Inspira-USA on April 27, 2022. Before he even started, Mr. Ahluwalia prepared a detailed service overview and business plan and strategy for Inspira-India cybersecurity services for the Americas, which he presented to Inspira-

India's leadership. Under his strategy, Mr. Ahluwalia planned to grow the Inspira-USA business by $90 million within five years based on an estimated investment by Inspira-India of $4.5 million.

36. As Inspira-USA's Chief Executive Officer and Inspira-India's Global Cybersecurity Head, Mr. Ahluwalia drove a major growth initiative to position Inspira-India and Inspira-USA for future success through the convergence of business, technology, and cybersecurity in collaboration with their customers. Mr. Ahluwalia led a go-to-market strategy for Inspira-India's cybersecurity services by bringing industry tailored and outcome based packaged services powered by iSMART2 framework to global customers through an integrated delivery model built on innovation and automation platforms and in close partnership with cybersecurity partners and alliances.

H. Proposed joint venture between Inspira-USA, Kintent Group, Inc. and CyberXForce

37. From September to early October 2022, Mr. Ahluwalia began leading discussions within Inspira-India and Inspira-USA for the purpose of analyzing various technologies that could be used to create Inspira-India's new solution service offering entitled "Digital CyberX Risk Management in the Box." After analyzing multiple different technologies offered by some of the leaders in the cybersecurity industry, the Inspira-India team selected Kintent Group, Inc. (Kintent) (now known as TrustCloud) as the technology developer for the "Digital CyberX Risk Management in the Box" solution offering. Kintent is a platform-based cybersecurity company based in Arlington, Massachusetts.

38. On or about November 1, 2022, Mr. Ahluwalia shared the project plan for configuring the technology with the Kintent and Inspira-India teams. On or about November 15, 2022, Mr. Ahluwalia shared in confidence with the Kintent and Inspira-India teams the first part

of CyberXForce's CyberXForce Technology consisting of the asset classification in a spreadsheet format.

39. On or about November 19, 2022, Mr. Ahluwalia traveled to India to meet in person with Prakash Jain—Chairman of the Board of Inspira-India. During their meeting, Mr. Ahluwalia explained to Mr. Prakash that Inspira-India had an opportunity to "disrupt the market" through its "Digital CyberX Risk Management in the Box" solution offering, which he explained would open the door for Inspira-India to provide all of its other service offerings to its customers. Mr. Ahluwalia told Mr. Prakash that since there is currently no technology on the market that can provide this solution (including any existing technology from Kintent), he offered to share his own intellectual property consisting of the CyberXForce Technology to power the "Digital CyberX Risk Management in the Box." Mr. Ahluwalia explained to Mr. Prakash that he would need to create a new entity called "CyberXForce" for purposes of entering into a letter of arrangement to form a joint venture between Inspira-India, Kintent and CyberXForce. Mr. Ahluwalia told Mr. Prakash that he would form this new entity once he returned to the United States November 27, 2022. Mr. Ahluwalia also told Mr. Prakash that Inspira-India would be the exclusive service provider and would benefit from the subscription fees charged to customers to use the platform. Mr. Prakash was interested in the idea and supportive of Mr. Ahluwalia's proposal to form this joint venture to create this new service offering for Inspira-India. After Mr. Ahluwalia's disclosure of this opportunity, Mr. Prakash expressed no interest in Inspira-India owning the CyberXForce Technology or acquiring equity in CyberXForce.

40. During his visit to India, Mr. Ahluwalia also met with Sachin Poptani—Inspira-India's Chief Legal Officer. During their discussion, Mr. Ahluwalia also shared with Mr. Poptani his discussions with Mr. Prakash about CyberXForce and his idea of "disrupting the market"

through the "Digital CyberX Risk Management in the Box" solution offering. Mr. Ahluwalia also described the solution, including the business imperatives, use cases, functions, and competitive advantage in the market. He also explained how the technology jointly developed by Kintent and CyberXForce would be used in the packaged solution offering. Mr. Poptani was receptive to the idea because, as Mr. Poptani explained, this proposal was already supported by Mr. Prakash. Shortly thereafter, Mr. Poptani began drafting a tri-party joint venture agreement (Letter of Engagement) between Inspira-USA, Kintent, and CyberXForce.

41. Upon his return to the United States, Mr. Ahluwalia filed the necessary documentation with the Delaware Secretary of State and formed CyberXForce Corporation on November 30, 2022.[1] After CyberXForce was formed, Mr. Ahluwalia permitted his company to use the CyberXForce Technology under an implied license.[2] Thus, CyberXForce is the owner of the trade secrets comprising the CyberXForce Technology because CyberXForce is the entity in whom or in which rightful, legal, or equitable title to, or the right to enforce rights in, the trade secret is reposed.

42. On or about December 7, 2022, Inspira-India, Mr. Ahluwalia and Mr. Poptani discussed in detail through telephone conferences and email communications about the draft Letter of Engagement and the joint venture between Inspira-USA, Kintent, and CyberXForce. In the draft

[1] Because the Letter of Engagement had not been finalized, Mr. Ahluwalia named his wife and mother—Nimmi Ahluwalia and Geeta Walia—as the initial directors of CyberXForce. Once it became clear that Mr. Ahluwalia would be signing the Letter of Engagement on behalf of CyberXForce, CyberXForce added Mr. Ahluwalia as a director.

[2] An implied license is an unwritten license which permits a party to do something that would normally require the express permission of another party. A license may be written, oral or implied. *Waymark Corp. v. Porta Sys. Corp.*, 334 F.3d 1358, 1364 (Fed. Cir. 2003); *Carborundum Co. v. Molten Metal Equip. Innovations, Inc.*, 72 F.3d 872, 878 (Fed. Cir. 1995). A license agreement is in essence nothing more than a promise by the licensor not to sue the licensee. *Carborundum Co.*, 72 F.3d at 878. Although most licenses are express, a license may be implied. *Id*. For example, the sale of a product that uses the patented invention results in an implied license. *Id*.

Letter of Engagement Mr. Poptani drafted and provided to Mr. Ahluwalia, Mr. Poptani explained that the purpose of the Letter of Engagement was to summarize the understanding between Inspira-USA, Kintent and CyberXForce to jointly develop the "Digital CyberX Risk Management in the Box" powered by Kintent's TrustCloud platform and CyberXForce's intellectual property around security risk management and Inspira-USA's connectors and iSMART2 framework. Mr. Poptani wrote "Inspira, Kintent, and CyberXForce are partnering together to jointly deliver an innovative and disruptive security and compliance solution for mid-market and enterprise customers to enable continuous, actionable, real-time assessments of their cybersecurity and compliance risks, help them achieve security and privacy compliance to multiple industry standards, and automated governance, analytics, and reporting process to manage their digital risk posture."

43. In the draft Letter of Engagement, Mr. Poptani drafted a provision providing that each party would "own[] and retain[] all right, title and interest, worldwide, in any and all of its intellectual property preexisting before the Effective Date of this [Letter of Engagement]." In addition, Mr. Poptani drafted another provision that stated the "[a]ll information and documents, whether oral or written or in electronic form, disclosed by one party to other parties pursuant to this [Letter of Engagement] shall be kept confidential by the receiving Party/ies ('Confidential Information')." Mr. Poptani also drafted a provision that "[n]one of the Parties will use the Confidential Information of the other Party/ies for purpose other than specified in this [Letter of Engagement]." Finally, Mr. Poptani drafted a provision stating that all Confidential Information would remain the exclusive property of the disclosing party and that under no circumstances would the Confidential Information be transferred, published or divulged to third parties without the prior written consent of the disclosing party. Multiple drafts of the Letter of Engagement containing these provisions were circulated between Mr. Ahluwalia, Mr. Poptani and Kintent.

44. Based on the Letter of Engagement, Defendants knew or should have known that the CyberXForce Technology provided by CyberXForce was a trade secret and the disclosure was made to them in confidence.

45. Based on this understanding, Mr. Ahluwalia began sharing certain confidential components of his CyberXForce Technology with the Kintent and Inspira-India teams in the form of detailed spreadsheet comprising CyberXForce's trade secret information, including security risk controls, control families and associated mapping and business and testing logic.

46. Unfortunately, during the course of the project, Kintent fell behind schedule and consistently delayed meeting certain milestones and deliverables outlined in the project plan. More concerning, an evaluation of the Kintent technology platform revealed it was very under-developed technology for the functions of the "Digital CyberX Risk Management in the Box" and would not at all be suitable or sophisticated enough to power the technology.

47. Due to Kintent's serious performance issues on the project, on or about December 15, 2022, Mr. Ahluwalia met with Inspira-India's platform engineering team and integrated cybersecurity services team to discuss whether it was time to look for an alternative to Kintent. In the meantime, Mr. Ahluwalia continue to share with the Inspira-India team the CyberXForce Technology for the teams to prepare interfaces to power a demonstration of the technology. CyberXForce confidentially shared its CyberXForce Technology in good faith with assurance from the Inspira-India leadership team that the parties would reach an agreement as early as January 2023.

48. Sometime during the latter part of January 2023, Mr. Ahluwalia had several discussions with Inspira-India board member Vishal Jain and Chief Legal Counsel Sachin Poptani about why Kintent's technology would not scale to enable the joint venture to complete the project.

Mr. Ahluwalia recommended that CyberXForce become the sole technology provider for the "Digital CyberX Risk Management in the Box" solution offering because the CyberXForce Technology was more advanced and was in the position to seamlessly replace Kintent to provide the power to enable the solution to work. They agreed, and Mr. Poptani began preparing a two-party agreement in the form of a joint development agreement between the Inspira-USA and CyberXForce. Mr. Poptani's draft joint development agreement contains virtually identical intellectual property and confidentiality provisions that he drafted in the Letter of Engagement.

49. Despite numerous discussions and meetings, Inspira-USA never reached an agreement with CyberXForce to use the CyberXForce Technology to power the "Digital CyberX Risk Management in the Box" solution offering or any other iSMART2 packaged offerings.

I. Termination

50. On April 3, 2023, shortly before his one-year anniversary and within days of being vested of his stock options in Inspira-India and Inspira-USA, Mr. Poptani and Mr. Vishal Jain flew from India to Texas and met Mr. Ahluwalia in a hotel lobby in Dallas, Texas. They informed Mr. Ahluwalia that he was being terminated for cause and handed him a termination letter. In the termination letter—signed by Mr. Prakash, Executive Chairman of Inspira-India—Mr. Ahluwalia was informed that he was terminated for cause due to a conflict of interest because he failed to disclose that he was involved in CyberXForce and that he attempted to cause Inspira-USA to enter into a Letter of Engagement with CyberXForce from which Mr. Ahluwalia and his family would have profited. By terminating Mr. Ahluwalia, Inspira-USA avoided having to pay Mr. Ahluwalia a substantial severance package and guaranteed vested stock options in Defendants.

J. Inspira-USA maliciously files a state court lawsuit against Mr. Ahluwalia and his companies.

51. On April 21, 2023, Defendant Inspira-USA filed an original petition and *ex parte* application for temporary restraining order against Mr. Ahluwalia, CyberXForce, DigitalXForce, and Mr. Ahluwalia's non-profit charitable organization, Inspire CyberX Excellence, Inc., in Cause No. 236-341752-23 styled *Inspira Enterprise, Inc.* v. *Lalit Ahluwalia, CyberXForce Corporation, Inspire CyberX Excellence, Inc., and DigitalXForce Corporation*, formerly pending in the 236th Judicial District, Tarrant County, Texas (State Court Litigation).

52. After conducting a hearing without any notice to Mr. Ahluwalia or Plaintiffs, the trial court granted an *ex parte* temporary restraining order against them. The trial court entered a temporary restraining order prohibiting Mr. Ahluwalia, his companies, and their respective agents, attorneys, representatives, affiliates and assigns, and any and all other persons under their control and/or direction, or acting in active concert and participation with them from (a) using or disclosing Inspira-USA's Confidential Information; (b) presenting Inspira-USA's Confidential Information, or similar iSMART2, or Digital CyberX products or marketing plan at the RSA Conference during April 24-27, 2023; or (c) soliciting, contacting, interfering, or otherwise communicating with Inspira-USA's clients or customers. The trial court further ordered that a hearing on the motion for temporary injunction would be held on May 5, 2023.

53. Mr. Ahluwalia had planned to launch the CyberXForce and DigitalXForce platforms at the RSA Conference—one of the largest cybersecurity conferences in the world. Because the trial court's temporary restraining order enjoined Mr. Ahluwalia and Plaintiffs from presenting this conference, Mr. Ahluwalia was forced to cancel his trip and cancel pre-scheduled meetings with potential clients, investors and business partners.

54. On information and belief, after obtaining the injunction, Defendants contacted Plaintiffs' future business partners and threatened them with cease and desist letters demanding that they stop conducting any business with Plaintiffs or they would be considered "co-conspirators." These false and damaging accusations severely damaged Plaintiffs business reputation, revenue and economic interests.

55. On April 28, 2023, Mr. Ahluwalia filed a motion to compel arbitration and plea of abatement regarding Inspira-USA's breach of contract and breach of fiduciary duty claims, which was set for hearing on May 5, 2023. Before the hearing, Plaintiffs sought to obtain the testimony of Inspira-USA's corporate representative and documents to prove that Mr. Ahluwalia and CyberXForce were owners of the CyberXForce Technology and that Mr. Ahluwalia and his companies did not use or disclose any of Inspira-USA's Confidential Information, or solicit any Inspira-USA customers. Plaintiffs also sought to forensically image a laptop computer believed to contain portions of CyberXForce's trade secrets. None of this discovery occurred because shortly before the hearing on the temporary injunction, Inspira-USA abruptly filed a nonsuit and dismissed the state court lawsuit without prejudice. As a result, Mr. Ahluwalia and Plaintiffs were unable to present undisputed evidence to the state court proving that the restraining order was wrongfully obtained.

E. Mr. Ahluwalia commences an arbitration proceeding pursuant to arbitration provision in the Employment Agreement.

56. After Inspira-USA dismissed the State Court Litigation, Mr. Ahluwalia commenced an arbitration proceeding against Inspira-USA under the parties' arbitration agreement on May 2, 2023. In the arbitration, Mr. Ahluwalia seeks to arbitrate a breach of contract claim and a declaratory judgment action against Inspira-USA. Mr. Ahluwalia specifically seeks significant monetary damages owed to him under his employment contract with Inspira-USA. He

also seeks a declaratory judgment declaring that he: (a) was terminated without cause; (b) did not breach his employment agreement with Inspira-USA; (c) did not use or disclose any "Confidential Information" in breach of his Confidential Information and Non-Disclosure Agreement with Inspira-USA; (d) did not breach his Non-Competition and Non-Solicitation Agreement with Inspira; and (e) did not breach any fiduciary duties.

57. As a result of Defendants' wrongful conduct, Defendants have caused irreparable damage to Plaintiffs and inhibited their ability to do business.

V. CLAIMS

COUNT I—Misappropriation of trade secrets by Defendants in violation of Texas Uniform Trade Secret Act (TUTSA) TEX. CIV. PRAC. & REM. CODE § 134A.001-.008 (2017) and the Defend Trade Secrets Act, 18 U.S.C. § 1836

58. Plaintiffs repeat and reallege each of the allegations contained in paragraphs 1-57 above.

59. CyberXForce owns certain trade secrets in connection with its CyberXForce technology including, but not limited to: integrated risk management business logic, technical and operational control assessment logic, asset inventory and attack surface management, security policies and plans review and generation, custom compliance, frameworks, interfaces, security tool connectors, artifacts, modules, source code, instances, security risk controls assessment analysis from NIST CSF and NIST 800-53 control families, and select security control mapping (CyberXForce Technology). CyberXForce took reasonable measures under the circumstances to keep its CyberXForce Technology secret. The CyberXForce Technology derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the CyberXForce Technology.

60. CyberXForce confidentially disclosed its CyberXForce Technology to Defendants as part of a joint venture in which CyberXForce expected to profit and which furthered its economic interests. Defendants knew or should have known that the CyberXForce Technology was a trade secret and the disclosure was made to them in confidence.

61. Defendants are willfully and maliciously misappropriating CyberXForce's trade secrets by disclosing and using the CyberXForce Technology without CyberXForce's express or implied consent, and that Defendants, at the time of the disclosure or use, knew or had reason to know that their knowledge of the trade secret was acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use.

62. As a result of Defendants' willful and malicious misappropriation of CyberXForce's trade secrets, CyberXForce is entitled to recover its actual damages it suffered as a result of the misappropriation including its lost profits, the development costs Defendants avoided by the misappropriation or the profits Defendants earned from their misappropriation under 18 U.S.C. § 1836 and TEX. CIV. PRAC. & REM. CODE § 134A.004, for which CyberXForce now sues.

63. CyberXForce also seeks an award of exemplary damages in an amount not to exceed twice its actual damages under TEX. CIV. PRAC. & REM. CODE § 134A.004 for Defendants' willful and malicious misappropriation.

64. In addition, CyberXForce seeks injunction relief under 18 U.S.C. § 1836(b)(3)(A) and TEX. CIV. PRAC. & REM. CODE § 134A.003 to enjoin Defendants' actual or threatened misappropriation.

COUNT II—Malicious prosecution.

65. Plaintiffs repeat and reallege each of the allegations contained in paragraphs 1-64 above.

66. Inspira-USA instituted a civil proceeding against Plaintiffs by or at the insistence of Defendants. Inspira-USA's injunction suit was commenced and prosecuted maliciously by Defendants based on ill-will, evil motive, or such gross indifference or reckless disregard for the rights of others as to amount to a willful and wanton act. Inspira-USA's injunction suit was commenced and prosecuted without probable cause. Inspira-USA later terminated the proceeding in Plaintiffs' favor because after Inspira-USA filed and set for hearing its application for temporary injunction, and after a motion to compel arbitration was filed and set for hearing, Inspira-USA withdrew its notice of hearing and terminated the proceeding. Inspira-USA did so to foreclose Plaintiffs' discovery, to avoid a procedural obstacle of the trial court compelling arbitration, and to escape an unfavorable ruling. As a result of Defendants' malicious prosecution, Plaintiffs suffered special injuries because the injunction restrained Plaintiffs from participating in an international industry conference to promote their cyber security technology, resulting in significant actual damages, including lost profits and reputational damages. Defendants are liable to Plaintiffs for the damages they sustained as a result of wrongful injunction, the reasonable and necessary expenses for defending the state court action, and exemplary damage, for which Plaintiffs now sue.

COUNT III—Wrongful injunction.

67. Plaintiffs repeat and reallege each of the allegations contained in paragraphs 1-66 above.

68. Inspira-USA filed an original petition and an *ex parte* application for temporary restraining order. The trial court granted Inspira-USA's application for temporary restraining order on the condition that it post a bond in the sum of $1,000 properly conditioned and securing the payment of such damages not to exceed said sum as may be sustained by any party who is

found to have been wrongfully restrained. That condition, as prescribed by Rule 684 of the Texas Rules of Civil Procedure, is "that the applicant will abide the decision which may be made in the cause, and that he will pay all sums of money and costs that may be adjudged against him if the restraining order or temporary injunction shall be dissolved in whole or in part." After Defendants obtained the temporary restraining order, but before the hearing on the temporary injunction, Defendants abruptly filed a nonsuit terminating the proceeding and the temporary injunction dissolved. Inspira-USA's nonsuit does not defeat Plaintiffs' right to sue for wrongful injunction.

69. Inspira-USA's temporary restraining order was issued when it should not have been, and it was later dissolved. Inspira-USA is therefore liable to Plaintiffs in the amount of $1,000 for the amount of the bond, for which Plaintiffs now sue.

COUNT IV— Defendants' tortious interference with Plaintiffs' prospective business relations.

70. Plaintiffs repeat and reallege each of the allegations contained in paragraphs 1-69 above.

71. Defendants intentionally interfered with Plaintiffs' prospective contractual or business relations. There is a reasonable probability that Plaintiffs would have entered into business relationships with customers interested in using the CyberXForce Technology. Defendants either acted with a conscious desire to prevent the relationships from occurring or knew the interference was certain or substantially certain to occur as a result of their wrongful conduct. Defendants misappropriated CyberXForce's trade secrets and used CyberXForce's advertising ideas and concepts using the CyberXForce Technology to promote Inspira-India's iSMART2 service offering without Plaintiffs' permission or authorization. Inspira-USA also maliciously prosecuted a lawsuit against Plaintiffs and others, wrongfully obtained an injunction,

and disparaged Plaintiffs to their business partners and customers, which caused substantial harm to Plaintiffs.

72. Defendants engaged in this tortious conduct with the desire to interfere with Plaintiffs' prospective contracts with their customers or with the belief that interference was substantially certain to result.

73. As a result of Defendants' tortious interference, Plaintiffs are entitled to recover their actual damages proximately caused by Defendants' interference, for which Plaintiffs now sue. In addition, because Defendants' interference was committed with malice, Plaintiffs also seek exemplary damages.

COUNT V—Business Disparagement

74. Plaintiffs repeat and reallege each of the allegations contained in paragraphs 1-73 above.

75. On information and belief, Defendants disparaged Plaintiffs' business by publishing—orally or in writing—disparaging false statements about Plaintiffs' business and their economic interests in the CyberXForce Technology to Plaintiffs' business partners, potential customers, and other third parties. On information and belief, the disparaging words cast doubt on CyberXForce's ownership of the CyberXForce Technology and suggested that anyone who did business with Plaintiffs would become a "co-conspirator." On information and belief, Defendants cast doubt on the propriety of Plaintiffs' business, their goods and services, and the character of their business, and reasonably imputed corporate dishonesty or other reprehensible conduct to Plaintiffs, or a third party reasonably understood the statements to cast this doubt. On information and belief, Defendants disparaging statements created a substantially false and defamatory impression by omitting material facts or juxtaposing facts in a misleading way. On information

and belief, when Defendants published the disparaging false statements, they knew the falsity of the statements, acted with reckless disregard of whether the statements were false, acted with ill-will, or intended to interfere with the economic interests of Plaintiffs. Defendants had no privilege or legal immunity protecting them when making these false and disparaging statements and allegations about Plaintiffs. On information and belief, Defendants' publication of the statements played a substantial part in inducing others not to do business with Plaintiffs. Defendants severely damaged and impacted Plaintiffs' business reputation, revenue, and economic interests resulting in pecuniary loss to Plaintiffs, including, actual damages, loss sales, lost profits, expense of reasonable measure to counteract the defamatory publication, and exemplary damages, for which Plaintiffs now sue.

VI. REQUEST FOR TEMPORARY RESTRAINING ORDER AND PRELIMINARY AND PERMANENT INJUNCTION

76. Plaintiffs repeat and reallege each of the allegations contained in paragraphs 1-75 above.

77. In accordance with Rule 65 of the Federal Rules of Civil Procedure and pursuant to 18 U.S.C. § 1836(b)(3)(A) and TEX. CIV. PRAC. & REM. CODE § 134A.003, Plaintiffs seek a temporary restraining order, a preliminary injunction, or in the alternative, a permanent injunction to enjoin Defendants' actual or threatened misappropriation.

78. Plaintiffs would show that they are entitled to a temporary restraining order and preliminary injunction because it can establish: (1) a substantial likelihood of success on the merits; (2) a substantial threat of irreparable injury if the injunction is not issued; (3) that the threatened injury if the injunction is denied outweighs any harm that will result if the injunction is granted; and (4) that the grant of an injunction will not disserve the public interest.

79. In the alternative, Plaintiffs would show they are entitled to a permanent injunction because they can demonstrate: (1) that they suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction.

80. There is a substantial likelihood of success on the merits because CyberXForce is the "owner" of the trade secrets comprising the CyberXForce Technology under DTSA and TUTSA. CyberXForce has an implied license to use the CyberXForce Technology and is the entity in whom or in which rightful, legal, or equitable title to, or the right to enforce rights in, the trade secret is reposed. 18 U.S.C. § 1839(4); TEX. CIV. PRAC. & REM. CODE § 134A.002.

81. CyberXForce took reasonable measures under the circumstances to keep its CyberXForce Technology secret. CyberXForce only disclosed the CyberXForce Technology to those who had a need to know it and who were under a duty of confidentiality. CyberXForce confidentially disclosed its CyberXForce Technology to Defendants as part of a joint venture in which CyberXForce expected to profit and which furthered its economic interests. Defendants knew or should have known that the CyberXForce Technology was a trade secret and the disclosure was made to them in confidence.

82. The CyberXForce Technology derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the CyberXForce Technology.

83. Defendants willfully and maliciously misappropriated CyberXForce's trade secrets by disclosing and using or threatening to disclose or use the CyberXForce Technology without

CyberXForce's express or implied consent, and that Defendants, at the time of the disclosure or use, knew or had reason to know that their knowledge of the trade secret was acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use.

84. There is a substantial threat of irreparable injury to Plaintiffs if the injunction is not issued. Defendants have misappropriated or threatened to misappropriate CyberXForce's trade secrets and will continue to do so in the absence of an injunction. Defendants have used or intend to use CyberXForce's trade secrets to launch a competing cybersecurity solution. Defendants misappropriated CyberXForce's trade secrets in direct violation of DTSA and TUTSA. Defendants have threatened irreparable harm to CyberXForce's intellectual property rights by using or threatening to use CyberXForce's trade secrets to sell and offer to sell to their customers and potential customers the iSMART2 service offering they claim is powered by the CyberXForce Technology.

85. Plaintiffs will suffer irreparable harm and damage if Defendants are permitted to discuss, present, or deliver the iSMART2 service offerings powered by CyberXForce Technology because once disclosed, Plaintiffs will lose their competitive advantage. Defendants should not be permitted to disclose, use, offer to sell, or sell any iSMART2 service offerings powered by the CyberXForce Technology without CyberXForce's explicit permission in the form of a license agreement or other similar agreement.

86. Moreover, Defendants will continue to use or threaten to use CyberXForce's trade secrets absent an injunction. Inspira-USA has also threatened to refile its state court lawsuit against Plaintiffs seeking another injunction to thwart Plaintiffs from selling and offering to sell their CyberXForce Technology, resulting in immediate harm to Plaintiffs.

87. As a result of Defendants' wrongful conduct, Plaintiffs have lost, and will continue to lose, potential customers and other business opportunities. The remedies available at law are inadequate to compensate for Plaintiffs' injuries because it would be impossible to determine how Defendants' misconduct has detrimentally affected Plaintiffs' businesses, and therefore Plaintiffs' damages are impossible to calculate. Plaintiffs are suffering, and will continue to suffer, irreparable harm by Defendants' actions unless this Court enjoins Defendants' actual and threatened misappropriation.

88. When considering the balance of hardships between Plaintiffs and Defendants, a temporary restraining order and preliminary and permanent injunctions are warranted. The harm to Plaintiffs far outweighs the harm to Defendants because Defendants will not be harmed if they are precluded from selling or offering for the iSMART2 service offering powered by the CyberXForce Technology owned by CyberXForce. The iSMART2 service offering is just one of the many service solutions offered by Defendants. Therefore, Defendants can still operate their business in the same manner they did before they misappropriated CyberXForce's trade secrets. Conversely, if an injunction is not entered, Plaintiffs will suffer and continue to suffer significant injury as a result of Defendants' brazen misappropriation of CyberXForce's trade secrets, and Plaintiffs' resulting loss of business and reputation in the market. The CyberXForce Technology, including its business logic and new methods for integrated risk management, could also be disclosed by Defendants to third party technology partners, who could then leverage the technology to unfairly compete against Plaintiffs. Defendants' disclosure would destroy any competitive advantage and do irreparable damage to Plaintiffs. Defendants are currently packaging "Digital CyberX Risk Management in the Box" into other service offerings such as "Security in the Box" and "Integrated Cyber Threat Management" and selling these service offerings to

customers and potential customers. As a result, Defendants are disclosing CyberXForce's business logic build into the CyberXForce Technology to customers and potential customers.

89. Finally, the public interest is always served when the Court ensures compliance with federal and state laws relating to trade secret and enjoins misappropriators. Protecting trade secrets does not disserve the public interest.

90. Defendants exploited Mr. Ahluwalia's talents, his knowledge and know-how, his substantial business contacts in the cybersecurity industry, and are now blatantly trying to steal his ideas and inventions by improperly using the United States court system to accomplish its illicit and corrupt goals.

91. For these reasons, Plaintiffs request that this Court enter a temporary restraining order, a preliminary and permanent injunction enjoining Defendants, and each of their officers, directors, employees, agents and affiliates and all those in active concert or participation with them from: (1) using or disclosing the CyberXForce Technology; (2) misrepresenting to customers and potential customers, analysts, Defendants' business and technology partners that Defendants have the right to disclose, use, offer to sell, or sell their iSMART2 service offerings (including, but not limited to the "Security in the Box," "Integrated Cyber Threat Management" and "Cyber Advisory" services and other associated services) powered by any CyberXForce Technology; (3) destroying or spoliating any evidence—including any evidence on any computers, servers or storage media—relating to CyberXForce or the CyberXForce Technology; and (4) refiling any state court proceeding that frustrates any federal right or remedy under DTSA or interferes in any way with this Court's jurisdiction or judgments.

92. Plaintiffs request that this Court further order that Defendants, their officers, directors, employees, agents, and affiliates and all those in active concert or participation with

them be commanded to (1) return to Plaintiffs any documents referring or relating to the CyberXForce Technology; and (2) file within ten (10) days of the date of the Court's Order a sworn declaration, signed under penalty of perjury, that it complied with this Court's Order;

VII. REQUEST FOR ATTORNEY'S FEES

Plaintiffs are entitled to recover their attorney's fees against Defendants for their willful and malicious misappropriation under Texas Civil Practice and Remedies Code §134A.005.

VIII. REQUEST FOR JURY TRIAL

1. Plaintiffs request a trial by jury.

PRAYER

For the reasons stated, Plaintiffs respectfully requests that this Court:

a. award their actual, compensatory, and special and exemplary damages as set forth above;

b. award exemplary damages in an amount not to exceed twice CyberXForce's actual damages under TEX. CIV. PRAC. & REM. CODE § 134A.004 for Defendants' willful and malicious misappropriation;

c. enter a temporary restraining order and preliminary and permanent injunctions enjoining Defendants, and each of their officers, directors, employees, affiliates, agents, and affiliates and all those in active concert or participation with them from: (1) using or disclosing the CyberXForce Technology; (2) misrepresenting to customers and potential customers, analysts, Defendants' business and technology partners that Defendants have the right to disclose, use, offer to sell, or sell their iSMART2 service offerings (including, but not limited to the "Security in the Box," "Integrated Cyber Threat Management" and "Cyber Advisory" services and other associated services) powered by any CyberXForce Technology; (3) destroying or spoliating any evidence—including any evidence on any computers, servers or storage media—relating to CyberXForce or the CyberXForce Technology; and (4) refiling any state court proceeding that frustrates any federal right or remedy under DTSA or interferes in any way with this Court's jurisdiction or judgments;

d. order that Defendants, their officers, directors, employees, affiliates, and agents and all those in active concert or participation with them be commanded to (1) return to Plaintiffs any documents referring or relating to the CyberXForce Technology; and (2) file within ten (10) days of the date of the Court's Order a sworn declaration, signed under penalty of perjury, that it complied with this Court's Order;

e. award Plaintiffs their reasonable attorney's fees;

f. award Plaintiffs' costs of court;

g. award Plaintiffs pre- and post-judgment interest at the highest amount allowed by law; and

h. enter such other and further relief that Plaintiffs may show themselves justly entitled.

Respectfully submitted,

/s/ *Joseph F. Cleveland, Jr.*
Joseph F. Cleveland, Jr.
Texas Bar No. 04378900
jcleveland@belaw.com
Angélique M. McCall
Texas Bar No. 24104172
amccall@belaw.com

BRACKETT & ELLIS
A Professional Corporation
100 Main Street
Fort Worth, TX 76102-3090
Telephone: 817/338-1700
Facsimile: 817/870-2265

ATTORNEYS FOR PLAINTIFFS

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document was sent to all parties and counsel of record pursuant to the Federal Rules of Civil Procedure and addressed as follows:

Via Private Service
Inspira Enterprise, Inc.
c/o its officers, managers or general agents or other agents authorized to receive service of process at
1301 Solana Boulevard, Suite 2570
Westlake, Texas 76262

Via Private Service
Inspira Enterprise, Inc.
c/o its Registered Agent
Chetan P. Prakash
2140 E. Southlake Blvd., Suite 803
Southlake, TX 76092

Via Private Service
Inspira Enterprise, Inc.
c/o its Registered Agent
National Registered Agents, Inc.
1209 Orange Street
Wilmington, Delaware 19801

Via Private Service
Inspira Enterprise India Limited
c/o its general agent,
Inspira Enterprise, Inc., or
Inspira Enterprise, Inc.'s officers, managers or other agents authorized to receive service of process at
1301 Solana Boulevard, Suite 2570
Westlake, Texas 76262

Via eMail and Hand Delivery
Cortney C. Thomas
Timothy B. Wells
BROWN FOX PLLC
8111 Preston Road, Suite 300
Dallas, Texas 75225
Phone: (214) 327-5000
Fax: (214) 327-5001
cort@brownfoxlaw.com
tim@brownfoxlaw.com

Via eMail and Overnight Delivery
Joseph Czerniawski
Appen Menon
CONDON & FORSYTH LLP
7 Times Square
New York, NY 10036
Phone: (212) 490-9100
Fax: (212) 370-4453
jczerniawski@condonlaw.com
amenon@condonlaw.com

DATED this May 5, 2023.

/s/ Joseph F. Cleveland, Jr.
Joseph F. Cleveland, Jr.

1547875-v1/17091-000200